Once errores comunes en la respuesta a incidentes cibernéticos

Cuando la integridad de una red informática o de un sistema de información se ve comprometida, responder adecuadamente y a tiempo minimiza las interrupciones en el negocio y reduce el impacto en las operaciones. En este sentido, existen once errores importantes que pueden obstaculizar la respuesta de las empresas a las violaciones de datos, ciberataques y otros eventos graves de seguridad informática. Ante ello, un programa proactivo e integral de respuesta a incidentes es un elemento crítico para la protección de la información y la continuidad de las operaciones.

Al evaluar un programa integral de respuesta a incidentes cibernéticos, se debe validar si este soluciona o empeora los problemas de seguridad, así como conocer las cualidades o aptitudes que tiene el equipo de respuesta para actuar de manera efectiva ante un incidente cibernético.

En la batalla impredecible contra los ciberatacantes, la preparación adecuada en los equipos de respuesta es un activo de valor para la empresa, pues estos desempeñan un papel clave en la seguridad de la información, la solución de problemas y el control de daños ante ataques informáticos.

Un programa proactivo e integral de respuesta a incidentes es un elemento crítico para la protección de la información y la continuidad de las operaciones

Abordar los once errores más comunes en el proceso de respuesta permite determinar si el equipo asignado para este fin es capaz de resolver, en lugar de exacerbar, los problemas de seguridad.

1 Planes que no están hechos a la medida de la empresa

Regularmente, las organizaciones implementan planes reutilizables de respuesta a incidentes en los que se enumera con gran detalle cada paso a tomar para investigar un posible incidente. Si bien esto podría parecer tranquilizador, a menudo complica los procedimientos de respuesta y ralentiza o afecta las investigaciones.

Los planes listos para usarse a menudo son obsoletos e ineficaces contra amenazas y tecnologías en constante evolución. Algunos elementos que no están considerados o cuya importancia se minimiza son: la incorporación de nuevas tecnologías que se transforman a ritmo acelerado; aspectos geográficos; cambios en el *modus operandi* de los cibercriminales; factores psicosociales, tecnológicos, culturales, así como de negocio y organización de la compañía.

Es fundamental que las organizaciones establezcan políticas, procesos y procedimientos adaptados a su cultura, entorno, personal de respuesta a incidentes, apetito de riesgo y, lo más importante, a sus objetivos de negocio. La documentación debe ser concisa y evolucionar constantemente para mantenerse al día respecto a dichos objetivos, las tendencias de la industria y los eventos políticos, culturales y sociales que puedan impactar a la empresa.

Planes que se activan únicamente cuando ocurre un incidente

Las empresas generan planes completos de respuesta ante incidentes que no son puestos a prueba sino hasta que se produce un evento real y, para entonces, se descubre que fallan desde el primer paso, lo cual demuestra que la planificación es insuficiente.

Además, numerosas organizaciones ven la creación de un plan de respuesta como un evento único, no como un proceso continuo. En consecuencia, los planes contienen información incorrecta sobre las personas que deben ser contactadas o las herramientas a utilizar, con pasos detallados que no funcionan o están fuera de lugar por no haberse actualizado ante algún cambio, proceso de maduración o fortalecimiento de las funciones.

En este sentido, las organizaciones deben probar sus planes con cierta regularidad, antes de que ocurra un incidente real, de la misma forma en que se hacen otro tipo de simulacros fuera del ambiente digital. Si carece de la realización de pruebas, el plan de respuesta a incidentes puede requerir un mayor tiempo de acción, generar confusión y, en el peor de los casos, permitir que un ataque sea exitoso, con un gran impacto negativo.

Comunicación inadecuada entre equipos y responsables

En ciertas áreas se suele trabajar en silos, y esto puede ser un desafío importante para identificar, coordinar y establecer comunicación con las partes clave involucradas en el proceso de respuesta a un incidente. Adicionalmente, dado que en este tipo de eventos el tiempo juega un papel crítico, los canales incorrectos o la falta de disponibilidad de información puede afectar de manera considerable la efectividad de la contención.

Sin duda, un repositorio centralizado de datos con el cual el equipo de respuesta pueda publicar detalles sobre la investigación en curso y, a la vez, extraer información según sea necesario, ayuda a limitar el impacto negativo de las constantes comunicaciones que se establecen por correo electrónico (exceso de correos, mensajes ignorados, información contradictoria). Además, se puede limitar el acceso a este repositorio o tablero de control (*dashboard*) o añadir a más personas de acuerdo con el avance en el proceso de respuesta.

Falta de habilidades técnicas, gestión inadecuada o personal insuficiente

Las organizaciones, independientemente de su tamaño, se enfrentan a distintos desafíos al elegir al personal que integra el equipo de respuesta a incidentes. Las más pequeñas frecuentemente cuentan con presupuestos de ciberseguridad limitados y suelen asignar estas tareas a los administradores de sistemas y redes, quienes poseen conocimientos técnicos pero pueden carecer de la experiencia, herramientas, habilidades y conocimientos para la gestión adecuada de los incidentes.

Asimismo, las corporaciones tienen dificultad al designar el número correcto o más eficiente de personas al equipo, pues se asume que más elementos equivalen a una mayor capacidad, lo cual puede llevar a que los esfuerzos se superpongan.

Por lo anterior, las organizaciones necesitan evaluar de forma detallada la necesidad de capacitación adicional o reclutamiento (interno o externo), que ayude a alcanzar el nivel adecuado de experiencia. También es fundamental identificar a terceros especializados que puedan proveer asistencia en ciertos aspectos del incidente o cuando este exceda las capacidades de respuesta, ya sea por lo crítico del problema o el tamaño y experiencia de la organización.

El liderazgo que supervisa al equipo tiene a su cargo definir claramente las funciones y responsabilidades de este, promoviendo una mayor colaboración y mejorando la comunicación dentro y fuera del equipo.

Destrucción de evidencia crítica

Comportamientos anómalos de equipos de cómputo, que podrían indicar un ciberataque, son reportados primero a la mesa de ayuda (*help desk*), incluyendo desde el bloqueo de cuentas del usuario hasta alertas de virus.

Si los miembros de dicha área no conocen los requerimientos de respuesta ante ciberataques, pueden destruir evidencia clave al tratar de solucionar los problemas del usuario; por ejemplo, instalar *software*, ejecutar antivirus o herramientas de limpieza, o ajustar la configuración del sistema puede sobrescribir información vital.

En estos casos, identificar la cadena de eventos de un incidente puede tornarse imposible, especialmente si las acciones iniciales no se documentaron. Por ello, las organizaciones deben asegurarse de que su personal de soporte técnico esté al tanto de los indicadores que necesitan la participación del equipo de respuesta a incidentes. Esto es de especial relevancia si se cuenta con el apoyo de empresas externas.

Si el personal de atención a usuarios sospecha que un problema reportado podría deberse a la presencia de un programa maligno, debe llevar a cabo una captura de imagen de la memoria del sistema antes de realizar cualquier cambio; asimismo, necesita recibir capacitación para documentar sus actividades en caso de que sus acciones formen parte de una investigación.

Por ello, es importante definir y transmitir a esta área los lineamientos a seguir y los parámetros que deben considerar antes de iniciar cualquier actividad, así como informar oportunamente de algún indicador que podría ser parte de otro evento de mayor magnitud.

Herramientas inadecuadas, mal administradas, no probadas o infrautilizadas

Se experimentan retrasos en los procesos de investigación y remediación de incidentes si las herramientas para obtener información de sistemas o usuarios afectados están mal administradas o subutilizadas. Si no existe una adecuada planeación, inversión, gestión, actualización y mantenimiento, incluso la solución tecnológica más avanzada puede fallar en cuanto a resultados confiables y consistentes.

Por ello, las empresas necesitan mantener un inventario de herramientas en una ubicación centralizada y establecer procesos que garanticen la renovación oportuna de licencias y actualizaciones de componentes funcionales.

Además, los miembros del equipo necesitan ser entrenados continuamente en todo el conjunto de herramientas, las cuales deben evaluarse periódicamente para determinar si pueden abordar las amenazas más actuales a las que se enfrenta la organización.

Información no disponible

Cuando la información que contiene los detalles relevantes de un ataque no existe o no está disponible fácilmente, hay un efecto en cascada durante todo el proceso de respuesta a incidentes. En última instancia, el equipo responsable tiene dificultades para evaluar el impacto, contener el daño y comunicar avances o resultados a la Dirección.

Abordar este problema implica comprender qué fuentes de datos se tienen, qué datos generan y cómo los pueden gestionar. La participación de los responsables de la tecnología y la existencia de un inventario de activos de información es necesaria para descubrir la gama de fuentes potenciales de datos.

Asimismo, el equipo de respuesta debe identificar eventos que proporcionen información acerca de un incidente y establecer procesos para la salvaguarda, agregación, almacenamiento y análisis de datos. Dichos eventos podrían incluir registros de autenticación fallida, eliminación de bitácoras, alertas antivirus, entre otros.

Estas actividades deben ser incluidas en la etapa de preparación como parte de un ciclo, ya que constantemente necesitan reevaluarse y ajustarse junto con las áreas operativas y de tecnología involucradas.

Falta de "inteligencia" en la inteligencia de amenazas

La inteligencia de amenazas (*threat intelligence*) es un tema de mucho interés, al punto que la oferta de soluciones y servicios asociados es muy amplia en el mercado de la seguridad de la información; sin embargo, muchas organizaciones descubren que, a pesar de comprar el acceso a todos los *feeds* disponibles, no siempre se logra una detección completa y oportuna de las amenazas. Con frecuencia, los equipos de respuesta a incidentes se encuentran abrumados con información técnica y otros indicadores, pero tienen poco o ningún contexto sobre cómo estos datos pueden afectar a la empresa.

Ante este desafío, resulta importante integrar la inteligencia de amenazas en la respuesta a incidentes y trabajar activamente con proveedores en la materia para determinar si lo que se está recibiendo es de valor para la compañía y puede realmente utilizarse. No basta con obtener mucha información: esta debe ser pertinente.

Poca autoridad y visibilidad del equipo de respuesta a incidentes

Las desavenencias políticas al interior de las organizaciones ejercen un efecto negativo en los esfuerzos del equipo de respuesta a incidentes; pueden, además, limitar la efectividad del proceso de reacción y evitar la resolución oportuna del problema. Además, es raro que dichos equipos operen con la autoridad suficiente para decidir sobre los cambios y acciones que deben tomarse y, más bien, deben escalar el asunto a la Dirección para recibir el apoyo necesario, en ocasiones a medida que la situación empeora.

La Dirección debe apoyar plenamente al equipo de respuesta, así como su misión y actividades durante una investigación. Asimismo, su función debe comunicarse y "venderse" como un servicio que mantiene la integridad de la empresa y no como algo que genera más trabajo. Dicho equipo necesita también involucrar a otros para designar un contacto que facilite la participación de las diversas áreas en el proceso de respuesta a incidentes (ver punto 2).

Vale la pena reiterar la importancia de la comunicación: saber "a quienes, qué y cómo" —lo cual debe ser definido previamente, permitiendo una respuesta más fluida y evitando toparse con personas que obstaculizan el proceso (*stoppers*). Un elemento importante dentro del flujo de comunicación es la posición organizacional del equipo, que debe gozar de cierta independencia y no estar adscrito al área de tecnología o sistemas.

Colaboradores que desconocen su papel en la seguridad

Aprovecharse de los usuarios finales es una de las formas más comunes y fáciles que utilizan los ciberdelincuentes para comprometer la seguridad de las organizaciones. A un atacante puede resultarle laborioso encontrar alguna vulnerabilidad que le otorgue acceso completo a una red, pero crear un mensaje de correo electrónico que convenza a un usuario de abrir el archivo o ingresar a una página maliciosa es mucho más sencillo y redituable. Desafortunadamente, instruir sobre estas amenazas no es tarea sencilla.

Los responsables de la seguridad de la información deben sensibilizar a los usuarios, no solo sobre las prácticas comunes utilizadas por ciberdelincuentes, sino también sobre su función como protectores de la información en la empresa. Lo anterior permite al personal participar activamente en temas de seguridad, saber a quién dirigirse y confiar en los procesos, en lugar de intentar resolver los problemas por su cuenta, incluso mediante la instalación de herramientas poco confiables, causando potencialmente mayores daños. La implementación de ejercicios periódicos que pongan a prueba el conocimiento, madurez y conciencia de los usuarios son un excelente medio para lograr estos propósitos.

Falta de aprobaciones

En ciertas situaciones, es necesario un análisis forense especializado como parte de la resolución de un incidente. Estos pueden requerir información que esté en computadoras personales o dispositivos móviles utilizados como parte de una política de "trae tu propio dispositivo" (BYOD, por sus siglas en inglés) o de terceros, especialmente proveedores de servicios de Tecnologías de la Información *in situ*. Con frecuencia, no se cuenta con el consentimiento previo de los usuarios de estos activos para recolectar la información requerida, lo cual afecta el avance del análisis y, en algunos casos, ocasiona la pérdida de evidencia digital relevante.

Ante este escenario, las empresas necesitan determinar, junto con sus asesores legales, las medidas previas (incluyendo modificaciones a contratos o firma de consentimiento adicionales) que les permitan el acceso a activos de información asignados a empleados o terceros. Estas deben contemplar situaciones en las que los colaboradores utilizan dispositivos personales para el trabajo, o en las que terceros y proveedores con equipos propios acceden a la red y recursos de la compañía; también debe considerar la revisión de los contratos y condiciones de los activos asignados al personal para su uso, como computadoras, teléfonos, tabletas, entre otros.

El valor de un apoyo personalizado

Con frecuencia, las compañías requieren apoyo especializado para la respuesta a incidentes cibernéticos y, en ciertos casos, que este actúe como extensión de los equipos internos. Desafortunadamente, no siempre se contempla esta posibilidad o se considera una vez que los problemas se han agravado.

Dado el riesgo de cibercrimen y las regulaciones en torno al tratamiento de datos personales, las organizaciones necesitan una visión oportuna de los problemas emergentes, así como asesoría práctica que ayude a proteger la información y asegurar el cumplimiento.

En este sentido, es necesario evaluar opciones que aporten un apoyo personalizado con base en una amplia experiencia en el sector donde opera la empresa, así como considerar el tamaño de la organización, los alcances y la complejidad del proyecto.

Todo lo anterior, favorece una opinión objetiva y una propuesta de solución adecuada a las características de cada compañía.

Los especialistas en respuesta a incidentes cibernéticos desarrollan constantemente herramientas y metodologías para abordar estos temas de forma cotidiana, haciendo frente a las diversas formas de delitos cibernéticos que sufren las empresas, como: amenazas internas, violaciones de datos, grupos *hacktivistas* e intrusiones del tipo "amenaza persistente avanzada" (APT, por sus siglas en inglés).

Con un enfoque pragmático y neutral, es posible incrementar la capacidad de la empresa para actuar ante incidentes informáticos de forma proactiva, asegurando la estabilidad del negocio.

kpmg.com.mx
800 292 KPMG (5764)
asesoria@kpmg.com.mx

KPMG MÉXICO
@KPMGMEXICO
KPMG MÉXICO
KPMGMX

Cuenta con 21 años de experiencia en materia forense, privacidad y seguridad de la información, asesorando a empresas de servicios financieros, farmacéutica, energía, entre otros sectores. Jefferson ha encabezado investigaciones forenses en países de Norteamérica, América Latina y Europa, en las que ha sido necesario identificar, preservar, recolectar, analizar y entregar evidencia digital, en casos relacionados con competencia desleal, malversación de activos, corrupción privada, cibercrimen, respuesta a incidentes cibernéticos y cumplimiento de la Ley de Prácticas de Corrupción en el Extranjero de Estados Unidos (FCPA, por sus siglas en inglés), entre otras. Jefferson también es especialista en regulaciones de privacidad en América Latina, y es miembro del consejo consultivo de (ISC)2 para la región desde 2011; cuenta con las certificaciones profesionales Cobit Foundation Certificate (CFC), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) y Certified Information Systems Security Professional (CISSP).

Si le interesa contactar al autor de este artículo o desea información adicional, favor de dirigirse al 800 292 5764, o si lo desea escríbanos a asesoria@kpmg.com.mx

Es posible que algunos o todos los servicios descritos en este documento no estén permitidos para los clientes de auditoría de KPMG y sus afiliados o entidades relacionadas.

SÚPER EMPRESAS EXPANSIÓN 2020 TOP companies

ESR Empresa Socialmente Responsable Inclusión Social

Norma Mexicana en Igualdad Laboral y No Discriminación